REMARKS

I. Introduction

In response to the Office Action dated September 25, 2007, which was made final, and in conjunction with the Request for Continued Examination (RCE) submitted herewith, claims 1 and 10 been amended. Claims 1-18 and 28-31 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Claim Amendments

Applicants' attorney has made amendments to the claims as indicated above to better distinguish the claims from the references. Support for these amendments can be found in the specification at least at page 12, line 1 et seq.

III. Prior Art Rejections

In pages 2-5 of the Office Action, claims 1-27 were rejected under 35 U.S.C. §103(a) as being obvious over the combination of U.S. Patent Publication No. 2001/0017920 (Son) and U.S. Patent Publication No. 2002/0001386 (Akiyama), as set forth below:

> 3. Claims 1-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record Son et al. (U.S. Patent Application Publication No. 2001/0017920, hereinafter "Son")) and further in view of Akiyama (US 200200001386)
>
> Claims 1,10 and 19, parts A through part D are anticipated by Son et al., elements 502- 516, figure 5B, where it is understood that a "copy protection key" can be any key to decode the program material within the client-slave set top box (AKA integrated receiver/decoder). paragraph 36 contains the detailed description of transferring both the copy protection key and the media to the client. Parts E and F are anticipated by elements 518-522.
>
> Son fails to teach c) means for encrypting the copy protection key at the host receiver using a host-client pairing key generated by the service prodder and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, wherein the service provider establishes the host-client pairing key for a particular combination the host and client receivers.
>
> However, in an analogous art Akiyama teaches (paragraph 0099) a conditional access system when each receiver apparatus has an individual master key. Akiyama teaches that [paragraph 0100] the conditional access system adopts a key configuration, as shown in, e.g., FIG. 3. More specifically, a work key Kw (i.e. a pairing key) which is specified for each channel and is common to all receiver apparatuses is encrypted using an individual master key KM, and the encrypted key is

sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent (see also paragraph 0101).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Akiyama into the method and system of Son for encrypting the copy protection key at the host receiver using a host-client pairing key generated by the service prodder and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, wherein the service provider establishes the host-client pairing key for a particular combination the host and client receivers, in order to prevent cryptanalysis and huge transmission volume caused by periodic changing of the channel key (protection key) as suggested by Akiyama (paragraph 0100)

Applicants' attorney respectfully traverses these rejections.

The Applicants' invention, as recited in amended independent claims 1 and 10, is patentable over the references, because it contains limitations not taught by the references. Neither of the references, taken individually or in combination, teach the same combination of elements as Applicants' claims, namely, a plurality of networked receivers, including at least one host receiver and at least one client receiver, and the steps or functions performed by those networked receivers when sharing encrypted program materials received from a service provider.

Consider, for example, the portions of Son cited by the Office Action, which are reproduced below:

Son: FIG. 5B

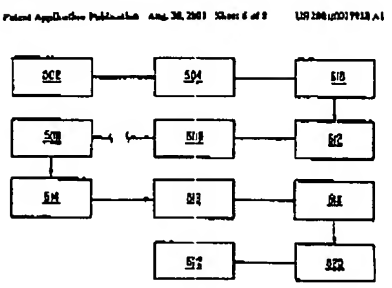

FIG. 5B

Son: Paragraphs [0033]–[0037]

[0033] FIG. 5B is a flow chart depicting a secure process for distributing video on-demand content via a cable distribution network in accordance with a second aspect of the present invention. The process depicted in FIG. 5B may be called a decrypt, re-encrypt, and store process. In comparison with the process in FIG. 5A, the process in FIG. 5B decrypts 510 and re-encrypts 512 the video program before the video program is stored 506 in the remote server 404.

[0034] First, a video program is encrypted 502 by a video on-demand source 402 to generate an encrypted program in a first encrypted form. The encrypted program is transported 504 via a primary distribution network from the video on-demand source 402 to a remote server 404 within a distribution center 106. At this point, the remote server 510 decrypts 510 the video program from the first encrypted form. A first key is may be used to accomplish such decryption 510, and such key may have been received from the video on-demand source 402 via a communication channel that is separate from the one used to transmit the video program. After the video program is decrypted 510, the remote server 404 re-encrypts 512 the video program into a second encrypted form using a second key. After the decryption 510 and re-encryption 510, the re-encrypted program is then stored 506 in the remote server 404.

[0035] Note that step 506 in FIG. 5B differs from step 506 in FIG. 5A in that step 506 in FIG. 5B involves storing the video program in the second encrypted form while step 506 in FIG. 5A involves storing the video program in the first encrypted form.

[0036] Subsequently, when the remote server 404 receives 508 a request for transmission of the video program from a subscriber station 110, the remote server

> 404 responds by multiplexing 514 the re-encrypted program in the second encrypted form (and the second key if necessary) with other signals to generate a multiplexed signal. The multiplexed signal is then distributed 516 via the secondary distribution network 108 to the requesting subscriber station 110.
>
> [0037] At the subscriber stations 110, the multiplexed signal is demultiplexed 518 to isolate the re-encrypted program in the second encrypted form (and the second key if necessary), the re-encrypted program is decrypted 520 from the second encrypted form to generate the unencrypted video program, and then the video program is displayed 522, typically, on a television monitor connected to set-top box.

Applicants' attorney submits that the above portions of Son do not teach or suggest a plurality of networked receivers, including at least one host receiver and at least one client receiver, that share encrypted program materials.

Instead, the above portions of Son merely describe a secure process for distributing video content on-demand, from a source through a server, which are part of the distribution system, to a subscriber station, which has only a single receiver. The video program is encrypted by the source, and then transported to the remote server within the distribution center. The remote server decrypts the video program from its first encrypted form using a key received from the source. The remote server then re-encrypts the video program into a second encrypted form using a second key, wherein the re-encrypted program in the second encrypted form (and the second key if necessary) is distributed to the requesting subscriber stations. At each of the subscriber stations, the re-encrypted program in the second encrypted form is decrypted using the second key, and displayed on a television monitor connected to set-top box.

However, nowhere do the above portions of Son describe a plurality of networked receivers, including at least one host receiver and at least one client receiver, and the steps or functions performed by those networked receivers when sharing encrypted program materials. Instead, only a single receiver can be found at the subscriber station.

Applicants' attorney also submits that these deficiencies of Son are not overcome by the Akiyama reference. Consider, for example, the portions of Akiyama cited by the Office Action, which are reproduced below:

Akiyama: FIGS. 3-5

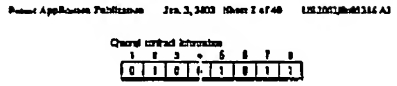

FIG. 2

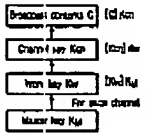

FIG. 3

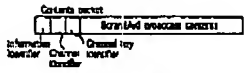

FIG. 4

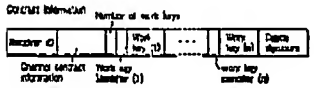

FIG. 5

Akiyama: Paragraphs [0099]–[0101]

[0099] The first embodiment is directed to a conditional access system when each receiver apparatus has an individual master key. Since such conditional access system must periodically and individually transmit encrypted control information containing channel contract information and the like to each receiver apparatus, the transmission volume of conditional access becomes large. However, since such system can assure high security (e.g., a narrow affected range upon breaking of the master key), CS broadcast and the like conventionally adopt such system. However, the volume of control information to be sent to each receiver apparatus becomes huge with increasing number of subscribers in recent years, and this embodiment provides solution for such problem.

[0100] The conditional access system adopts a key configuration, as shown in, e.g., FIG. 3. More specifically, a work key Kw which is specified for each channel and is common to all receiver apparatuses is encrypted using an individual master key KM, and the encrypted key is sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent. Since broadcast contents are encrypted by a conventional cryptography technique, they can be decrypted using that channel key. Note that the channel key must normally be changed at short periods (e.g., 10 min) to prevent cryptanalysis. If an individual master key is used to send this channel key, the transmission volume becomes huge. For this reason, a work key common to all receiver apparatuses must be used. Since it is dangerous to use an identical work key for several months, that key must also be changed, and is encrypted using an individual master key. Hence, even when the master key is known, free subscription can be prevented by changing the work key.

> [0101] Data to be received by the broadcast receiver apparatus via a broadcast wave in the conditional access system of this embodiment include two different packets, i.e., a contents packet and common control packet. The contents packet has a packet format shown in FIG. 4, and includes an information identifier (packet identifier), channel identifier, channel key identifier, and scrambled broadcast contents (encrypted using a channel key).

Applicants' attorney submits that the above portions of Akiyama do not teach or suggest a plurality of networked receivers, including at least one host receiver and at least one client receiver, and the steps or functions performed by those networked receivers when sharing encrypted program materials.

Instead, the above portions of Akiyama merely describe a method of sharing keys among receivers in a conditional access system. Specifically, Akiyama describes the use of a work key Kw, which is specified for each channel and is common to all receivers, which is encrypted using an individual master key KM, which is also associated with all receivers, and a channel key Kch, which is encrypted using the work key Kw. Thereafter, broadcast contents, which are encrypted, can be decrypted by the receiver using the channel key. Both the channel key and the work key are changed periodically, where the channel key is changed more often than the work key.

However, nowhere do the above portions of Akiyama describe a plurality of networked receivers, including at least one host receiver and at least one client receiver, and the steps or functions performed by those networked receivers when sharing encrypted program materials. Instead, each subscriber has only a single receiver.

Therefore, even when combined, the Son and Akiyama references do not teach or suggest all the limitations of Applicants' claimed invention. Moreover, the various elements of Applicants' claimed invention together provide operational advantages over the combination of Son and Akiyama. In addition, Applicants' invention solves problems not recognized by the combination of Son and Akiyama.

Thus, Applicants' attorney submits that independent claims 1 and 10 are allowable over Son and the combination of Son and Akiyama. Further, dependent claims 2-9, 11-18, and 28-31 are submitted to be allowable over the combination of Son and Akiyama in the same manner, because they are dependent on independent claims 1 and 10, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-9, 11-18, and 28-31 recite additional novel elements not shown by the combination of Son and Akiyama.

IV. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited.

Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP

Attorneys for Applicant

Date: December 18, 2007

By: _____

Name: George H. Gates

Reg. No.: 33,500

GHG/